UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MARK ROBINSON, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. **MAINTECH INC. and MAINTECH, INCORPORATED**, Defendant.	**CASE NO. 2:23-cv-4458** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff MARK ROBINSON ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant MAINTECH INC. and MAINTECH, INCORPORATED, (collectively, "Maintech" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, driver's license, and financial information ("personally identifying information" or "PII").

3. Maintech's breach differs from typical data breaches because it affects consumers who had no relationship with Maintech, never sought one, and never consented to Maintech collecting and storing their information.

4. Maintech sourced their information from third parties, stored it on Maintech's systems, and assumed a duty to protect it, advertising that it is "commit[ed] to protecting your privacy and personal information."[1] But Maintech never implemented the security safeguards needed despite acknowledging their importance.

5. On information and belief, the Data Breach occurred on January 29, 2023. However, Maintech struggled to identify what information was information was involved, and, on information and belief, did not do so until June 20,2023, an appalling six months later.

6. On July 13, 2023, Maintech finally began notifying Class Members about the widespread Data Breach ("Notice Letter"), an example of which is attached as Exhibit A. However, Maintech has not completed notification of Class Members and continues to do so.

7. Maintech waited almost seven months before informing Class Members even though Plaintiff and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. Maintech's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened,

[1] Privacy Policy, Maintech, https://www.maintech.com/terms-of-use-privacy-policy/ (last visited August 9, 2023).

or why it took Maintech almost seven months to begin notifying victims that hackers had gained access to highly sensitive PII.

9. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

10. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

11. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its consumers.

12. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff Mark Robinson is a Data Breach victim.

14. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

15. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, consumers' private information was exactly that—private. Not anymore. Now, consumers' private information is forever exposed and unsecure.

PARTIES

16. Plaintiff, Mark Robinson, is a natural person and citizen of Delaware, where he intends to remain. Plaintiff is a Data Breach victim, receiving the Breach Notice on July 19, 2023.

17. Defendant, Maintech Inc., is a Delaware Corporation, with its principal place of business at 14 Commerce Dr #200, Cranford, NJ 07016. Defendant is a citizen of Delaware and New Jersey.

18. Defendant, Maintech, Incorporated, is a Delaware Corporation, with its principal place of business at 14 Commerce Dr #200, Cranford, NJ 07016. Defendant is a citizen of Delaware and New Jersey.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one Class Member and Defendant are citizens of different states.

20. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Maintech

22. Maintech provides support and IT consultation and support to a "global market", serving customers ranging from mid-size companies to global BFSI entities in 50+ countries.[2] Maintech boasts a total annual revenue of $300 million. [3]

23. As part of its business, Defendant receives and maintains the PII of thousands of consumers (such as, *inter alia*, its clients' consumers) In collecting and maintaining PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII.

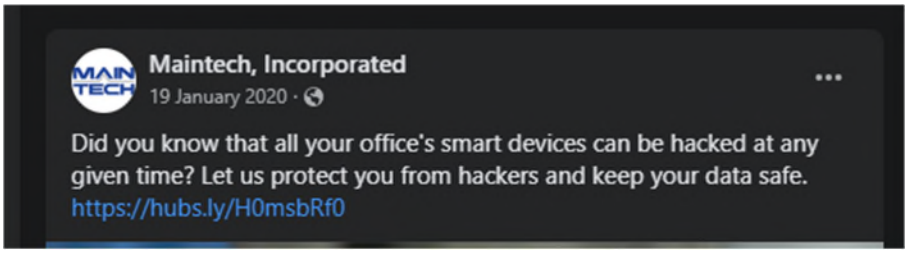
24. Indeed, Maintech boasts that as "experts," it has "over 40 years of experiencing working alongside leading companies in high-demand fields"[4], promising that it is "commit[ed] to protecting your privacy and personal information."[5]

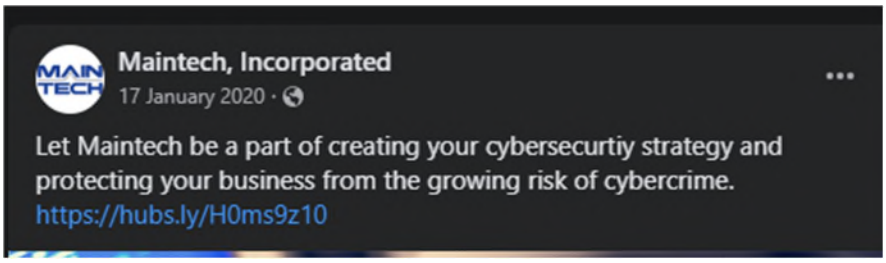
25. Maintech assures its consumers that "to insure that your PII and Registration Data are secure, Maintech stores all data in an encrypted database that complies with a complex authentication process."[6]

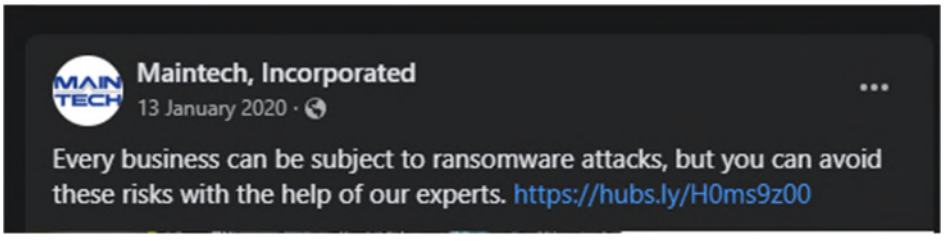
26. So confident is Maintech in its ability to protect and "insure" consumers' PII, that it released an article warning that "billions of records were exposed by data breaches in 2019 alone. Don't let your business become a statistic in cybersecurity- contact us today."

[2] About us, Maintech, https://www.maintech.com/about/ (last visited August 10, 2023).
[3] Maintech, Zoominfo, https://www.zoominfo.com/c/maintech-inc/23561084 last visited August 10, 2023).
[4] About Us, Maintech, https://www.maintech.com/about/ (last visited August 10, 2023).
[5] Privacy Policy, Maintech, https://www.maintech.com/terms-of-use-privacy-policy/ (last visited August 10, 2023).
[6] *Id*.

27. Indeed, Maintech regularly warns clients of the risks of data breaches, positioning itself as experts in cybersecurity through a plethora of posts:







28. In collecting and maintaining consumers' PII, Maintech agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

29. Despite recognizing its duty to do so, on information and belief, Maintech has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Maintech leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

30. Plaintiff is unsure how Maintech got his information but assumes that one of Maintech's clients he utilizes provided Maintech with his personal information including but not limited to his name, driver's license, financial information, and Social Security Number.

31. On information and belief, Defendant collects and maintains consumers' PII in its computer systems.

32. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

33. According to the Breach Notice, Maintech "became aware of certain unauthorized activity within its computer systems" on January 29, 2023. Following an internal investigation, Maintech discovered that "personal information may have been accessed by an unauthorized third party in connection with this incident." Ex. A.

34. In other words, despite claiming to be experts in cybersecurity, Maintech's investigation revealed that Defendant's cyber and data security systems were completely

inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly sensitive PII.

35. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

36. On or around July 13, 2023, –almost seven months after the Breach first occurred– Maintech finally began notifying Class Members about the Data Breach.

37. Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

38. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

39. In response to the Data Breach, Defendant contends that it has or will be taking "steps to address the incident and is committed to protecting personal information in its care" Ex. A. Although Defendant fails to expand on what these alleged "steps" are, such steps should have been in place before the Data Breach.

40. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity". Ex. A.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other

sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, Maintech has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

43. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

45. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the industries Defendant provides services to, including manufacturing and financial industries, preceding the date of the breach.

46. In light of recent high profile data breaches, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[7] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[8]

48. Indeed, cyberattacks against the financial and manufacturing industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [9]

49. Defendant itself issued a plethora of warnings regarding the rising number of data breaches in industries that Defendant offered IT services, including cybersecurity, for.[10]

50. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Maintech.

Plaintiff's Experience

51. Plaintiff Robinson received the Maintech's Breach Notice on July 19, 2023. He is unsure why Defendant is in possession of his PII but assumes it was provided by one of Maintech's clients that he utilizes.

---

[7] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 13, 2023).
[8] *Id*.
[9] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 13, 2023).
[10] Maintech, Facebook, https://www.facebook.com/maintech1 (last visited August 10, 2023).

52. Regardless, Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

53. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

54. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over three months.

55. Indeed, following the Data Breach, Plaintiff was contacted by TD Bank, informing him that his debit card was subject to four fraudulent attempts to charge him from four different states that Plaintiff did not authorize. These fraudulent charges ranged from 1 cent to $1.15 and suggests that Plaintiff's PII is now in the hands of cybercriminals.

56. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

57. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

58. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

59. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

60. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

61. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

62. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

63. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

64. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

65. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

66. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

67. One such example of criminals using PII for profit is the development of "Fullz" packages.

68. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

70. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

71. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

72. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued

numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

75. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

76. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

78. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

79. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

80. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

81. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

82. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its consumers. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

83. Plaintiff sues on behalf of himself and the proposed class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose PII was compromised in the Maintech Data Breach, including all those who received notice of the breach.

84. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

85. Plaintiff reserves the right to amend the class definition.

86. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least thousands of individuals who have been damaged by Defendant's conduct as alleged herein.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

    i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

    ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

    iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

    iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

    v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

87. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

88. Plaintiff realleges all paragraphs as if fully set forth below.

89. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

90. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing

to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

91. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

92. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's PII.

93. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

94. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

95. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing

to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

96. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

97. Plaintiff realleges all paragraphs as if fully set forth below.

98. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

99. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII. The FTC publications and orders promulgated pursuant to the

FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

100. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

101. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

102. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

103. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

104. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

105. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

106. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

107. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

108. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

109. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class)

110. Plaintiff realleges all paragraphs as if fully set forth below.

111. Defendant entered into various contracts with its clients, to provide IT services to its clients.

112. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

113. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

114. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

115. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

116. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

117. Plaintiff realleges all paragraphs as if fully set forth below.

118. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide IT services.

119. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII, as this was used to provide IT services.

120. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

121. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

122. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

123. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII.

124. Plaintiff and Class members have no adequate remedy at law.

125. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

126. Plaintiff realleges all paragraphs as if fully set forth below.

127. In light of the special relationship between Defendant Maintech and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

128. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Maintech's relationship with its, in particular, to keep secure their PII.

129. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

130. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

131. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

132. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

133. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

134. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, *et seq.*
(On Behalf of Plaintiff and the Class)

135. Plaintiff realleges all paragraphs as if fully set forth below.

136. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, *et seq.*, prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

137. Plaintiff, Defendant, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

138. Defendant sells "merchandise," as defined by N.J.S.A. § 56:8-1, by offering IT and cybersecurity services to the public.

139. Defendant, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of IT and cybersecurity services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of IT services, to its clients' consumers, including the Plaintiff and Class Members, by representing that they would maintain adequate data security practices and procedures to safeguard Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of IT services, to its clients' consumers, including the Plaintiff and Class Members, by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII with the intent that Plaintiff and Class Members rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of IT and cybersecurity services by failing to maintain the privacy and security of Plaintiff's and Class Members' PII in violation of duties imposed by and public policies reflected in the FTC Act;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Representing on its website that it is "commit[ed] to protecting your privacy and personal information," when, in fact, Maintech never implemented the security safeguards needed.

140. The above unlawful and deceptive acts and practices by Defendant was immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

141. Defendant knew or should have known that their data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach was highly likely. Defendant's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

142. Plaintiff and Class Members reasonably expected that Defendant would protect their PII and reasonably expected that Defendant would provide truthful statements on their website and privacy policies, and that it would be safe to provide Maintech with their information. These representations and affirmations of fact made by Defendant, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to entrust their information to Maintech. Defendant, moreover, intended for consumers, including Plaintiff and Class Members, to rely on these material facts.

143. As a direct and proximate result of Defendant's unconscionable and deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

144. Plaintiff and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: August 14, 2023

Respectfully submitted,

By: */s/ Patrick Howard*

Patrick Howard (NJ Atty ID #02280-2001)
Simon B. Paris (NJ Atty ID #04982-1996)
SALTZ MONGELUZZI & BENDESKY, P.C.

8000 Sagemore Drive, Suite 8303
Marlton, NJ 08053
Tel: (856) 751-0868
phoward@smbb.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class